

ローカル LAN への AnyConnect クライアントアクセスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[背景説明](#)

[AnyConnectセキュアモビリティクライアントのローカルLANアクセスの設定](#)

[ASDM 経由での ASA の設定](#)

[CLI による ASA の設定](#)

[Cisco AnyConnect セキュア モビリティ クライアントの設定](#)

[ユーザ設定](#)

[XML プロファイルの例](#)

[確認](#)

[Cisco AnyConnect セキュア モビリティ クライアント](#)

[Ping でローカル LAN アクセスをテストする](#)

[トラブルシューティング](#)

[名前による印刷またはブラウズができない](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco AnyConnect セキュア モビリティ クライアントが、Cisco ASA への接続中にローカル LAN にアクセスできるようにする方法について説明します。

前提条件

要件

このドキュメントでは、機能しているリモートアクセスVPN設定がCisco適応型セキュリティアプリケーション(ASA)にすでに存在していることを前提としています。

必要に応じて、『[CLIブック3: Cisco ASAシリーズVPN CLIコンフィギュレーションガイド9.17](#)』の設定を参照してください。

使用するコンポーネント

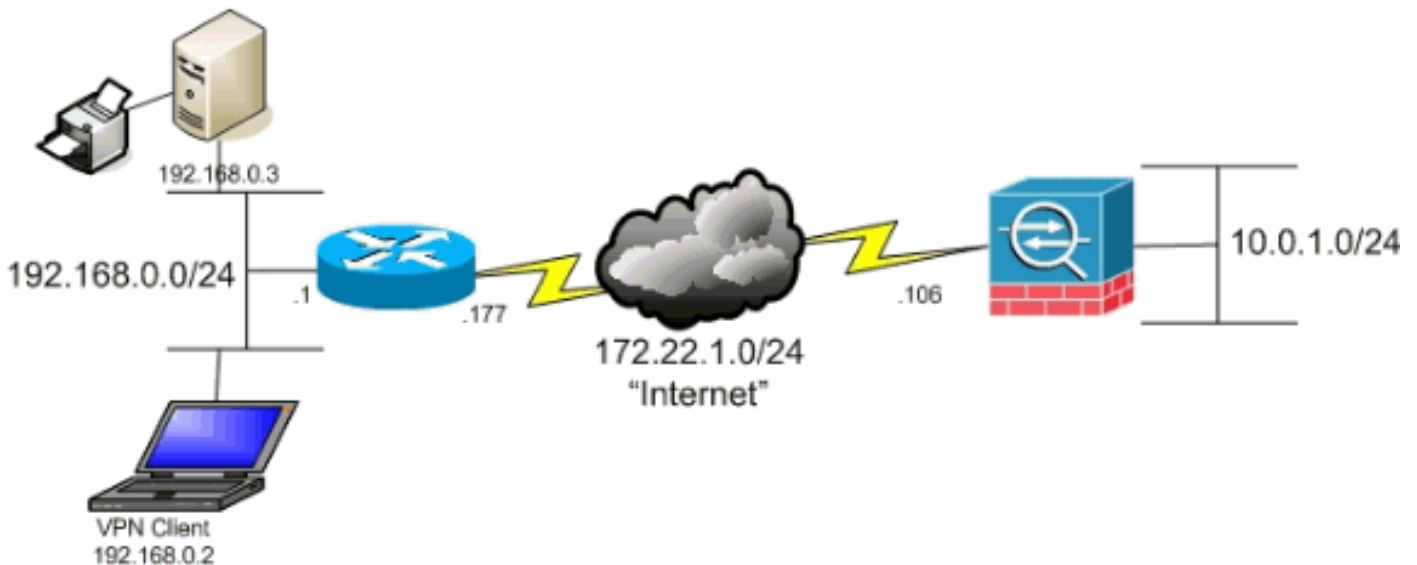
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA 5500 シリーズ バージョン 9(2)1
- Cisco Adaptive Security Device Manager (ASDM) バージョン 7.1(6)
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 3.1.05152

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図

クライアントは一般的なスモールオフィス/ホームオフィス (SOHO) ネットワーク上にあり、インターネット経由で本社に接続しています。



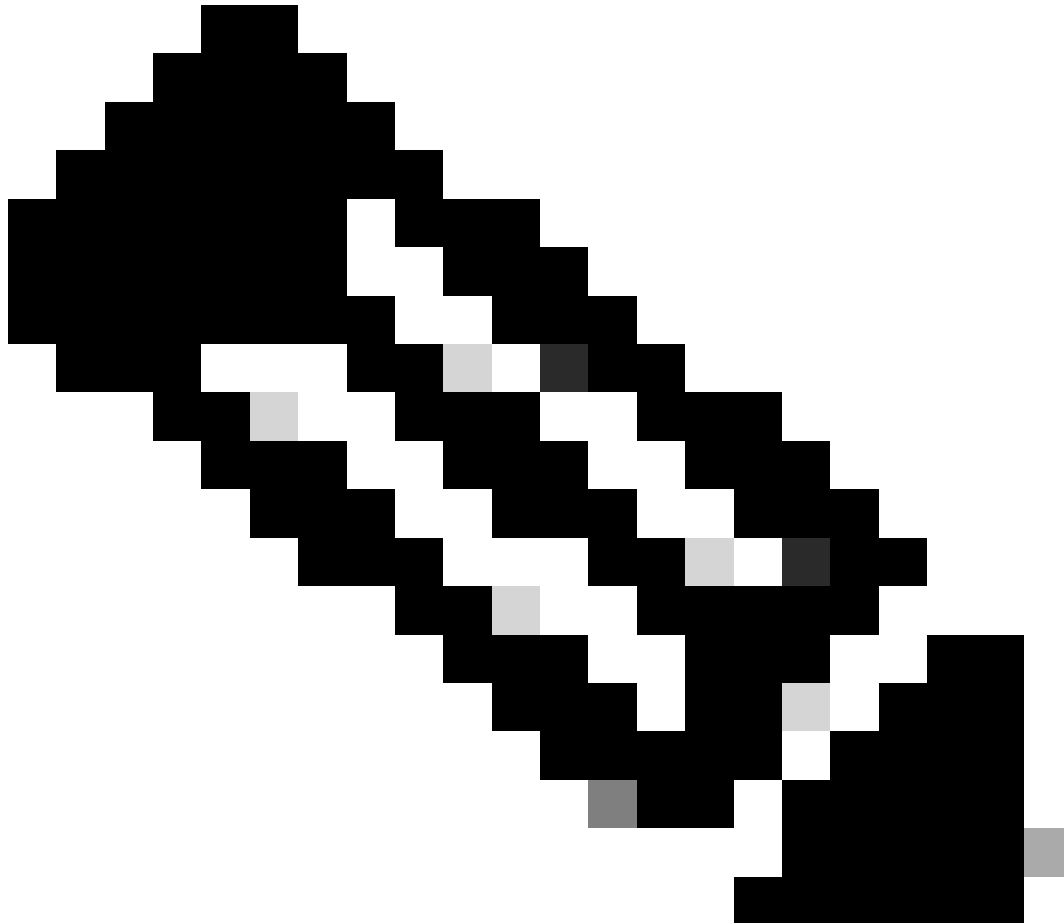
背景説明

この設定により、Cisco AnyConnectセキュアモビリティクライアントは、IPsec、Secure Sockets Layer(SSL)、またはInternet Key Exchange Version 2(IKEv2)を介して企業リソースへの安全なアクセスが可能になり、クライアントが配置された場所への印刷などのアクティビティを実行する機能もクライアントに提供されます。許可されている場合、インターネット宛てのトラフィックは引き続き ASA にトンネリングされます。


すべてのインターネットトラフィックが暗号化されずに送信される従来のスプリットトンネリングシナリオとは異なり、VPNクライアント用にローカルのLANアクセスを有効にすると、それらのクライアントは、存在する場所のネットワーク上にあるデバイスだけと暗号化せずに通信することを許可されます。たとえば、自宅からASAに接続しながらローカルLANアクセスを許可されているクライアントは、自分のプリンタに出力することはできますが、インターネットにアクセスするには、まずトンネル経由でトラフィックを送信する必要があります。

ASAでスプリットトンネリングを設定する場合とほぼ同じように、ローカルLANアクセスの許可には、アクセスリストが使用されます。ただし、スプリットトンネリングのシナリオとは異なり、このアクセスリストでは、暗号化する必要があるネットワークが定義されません。代わりに

、暗号化しないネットワークを定義します。また、スプリット トンネリング シナリオとは異なり、リスト内の実際のネットワークを知る必要はありません。その代わりに、ASA は、クライアントのローカル LAN を意味すると理解されているデフォルト ネットワークの 0.0.0.0/255.255.255.255 を供給します。



注：これは、クライアントがASAに接続されている間にインターネットに暗号化されていないアクセスを行うスプリットトンネリングの設定ではありません。ASAでスプリットトンネリングを設定する方法については、『[CLIブック3: Cisco ASAシリーズVPN CLIコンフィギュレーションガイド9.17](#)』の「スプリットトンネリングポリシーの設定」を参照してください。

 注：クライアントがローカルLANアクセス用に接続および設定されている場合、ローカルLAN上で名前による印刷または表示はできません。ただし、IP アドレスによる表示や印刷は可能です。この状況の詳細および回避策については、このドキュメントの「[トラブルシューティング](#)」セクションを参照してください。

AnyConnectセキュアモバイルクライアントのローカルLANアクセスの設定

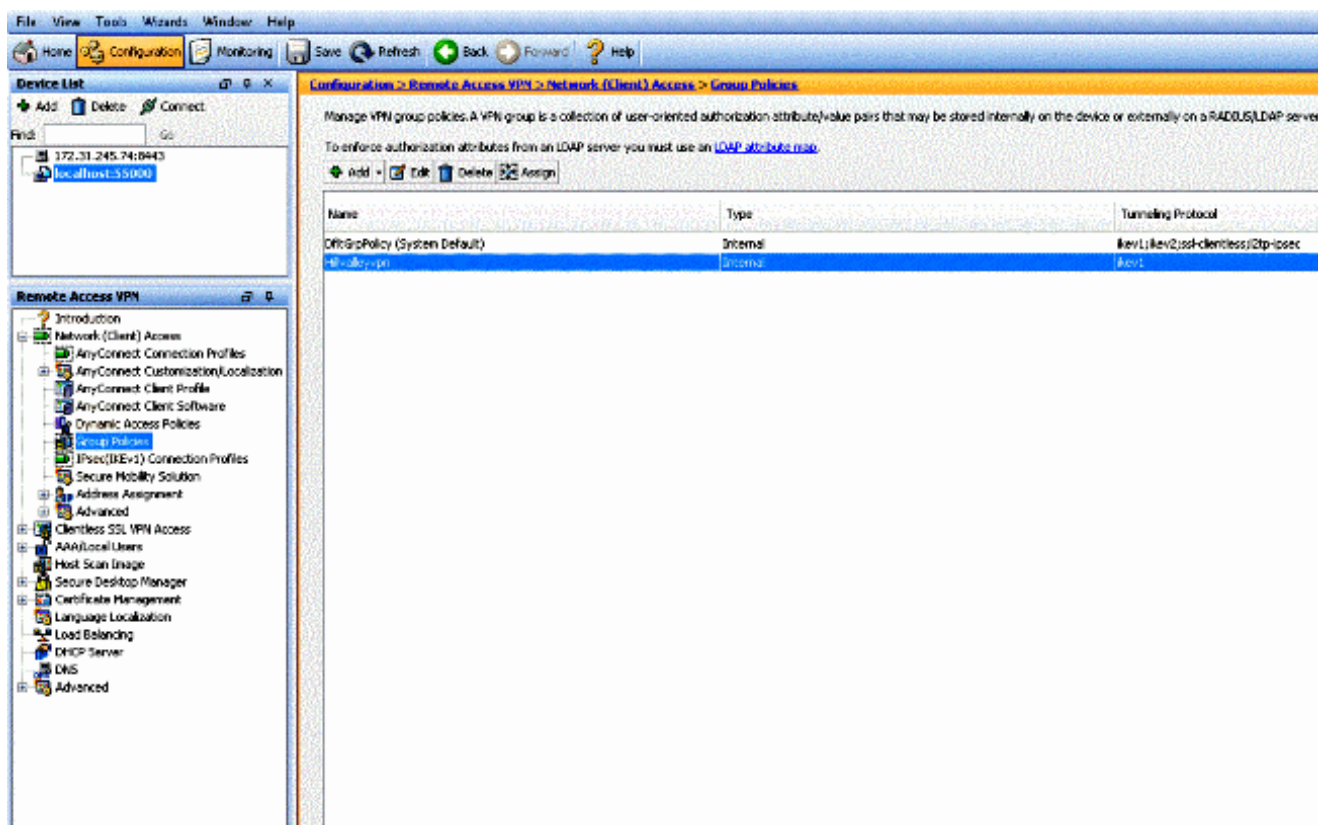
ASAへの接続中にCisco AnyConnectセキュアモバイルクライアントがローカルLANにアクセスできるようにするには、次のタスクを実行します。

- [ASDM 経由での ASA の設定または CLI による ASA の設定](#)
- [Cisco AnyConnect セキュア モバイルクライアントの設定](#)

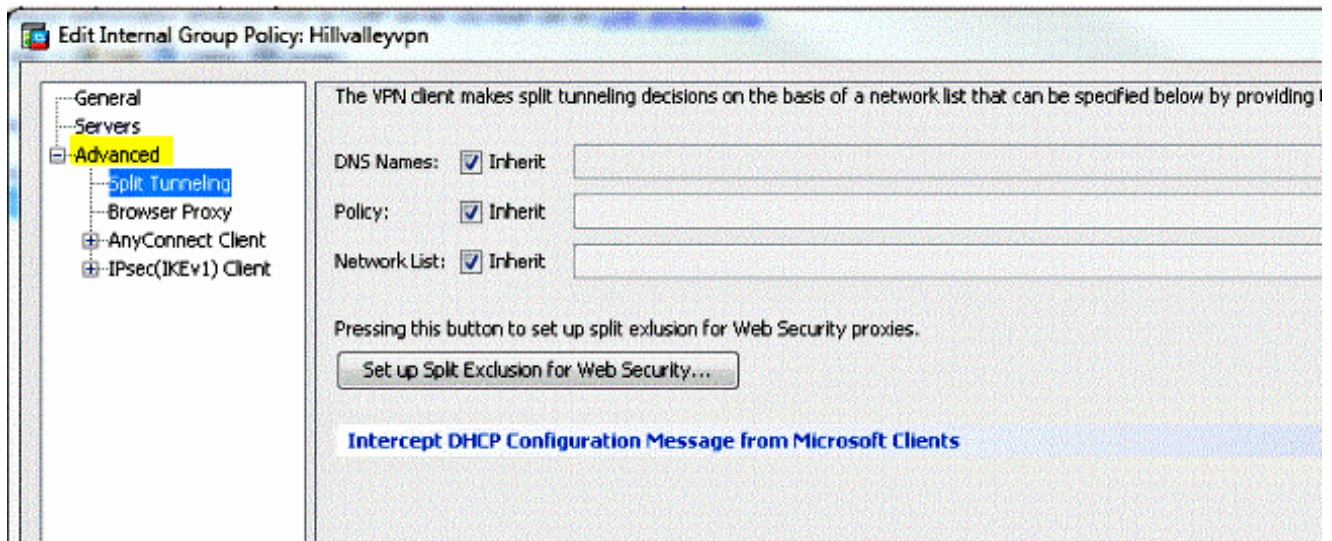
ASDM 経由での ASA の設定

ASA に接続しながら、VPN Client にローカル LAN アクセスを許可するには、ASDM で次の手順を実施します。

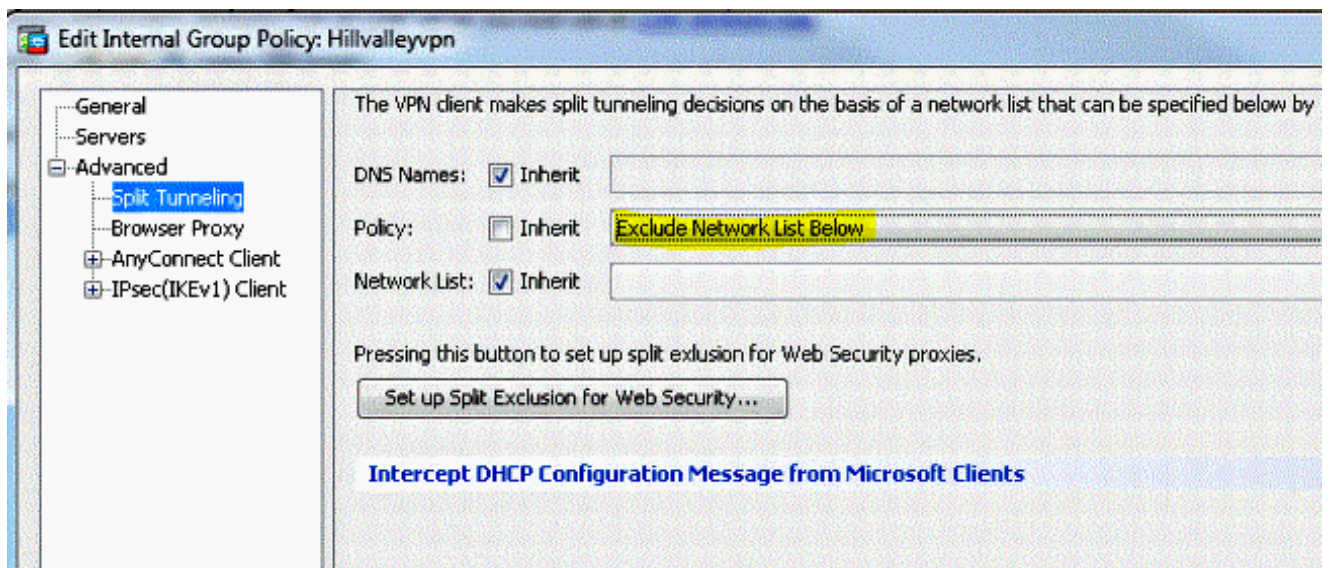
1. **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** を選択し、ローカルLANアクセスをイネーブにするグループポリシーを選択します。次に、**Edit**をクリックします。



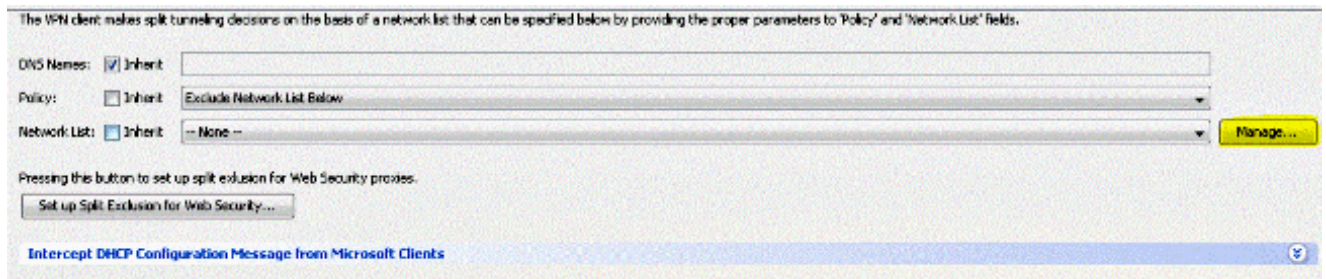
- 次に、Advanced > Split Tunneling



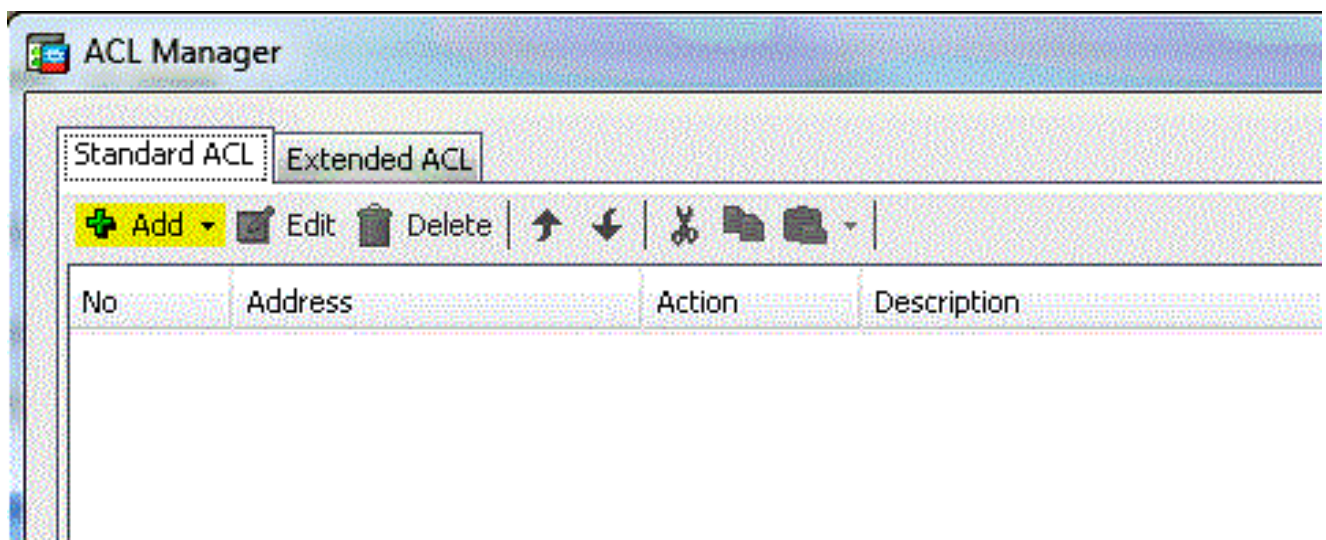
- Policyの **Inherit** ボックスのチェックマークを外し、**Exclude Network List Below**を選択します。



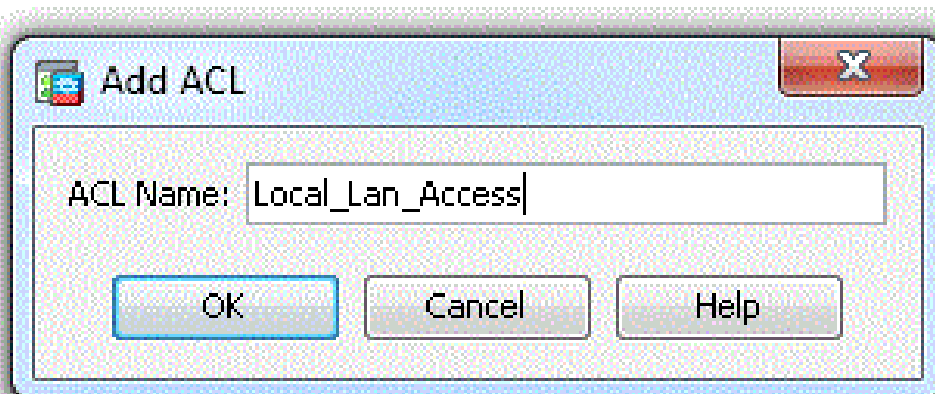
- Network Listの **Inherit** ボックスのチェックマークを外し、**Manage** し、をクリックしてAccess Control List (ACL ; アクセスコントロールリスト) Managerを起動します。



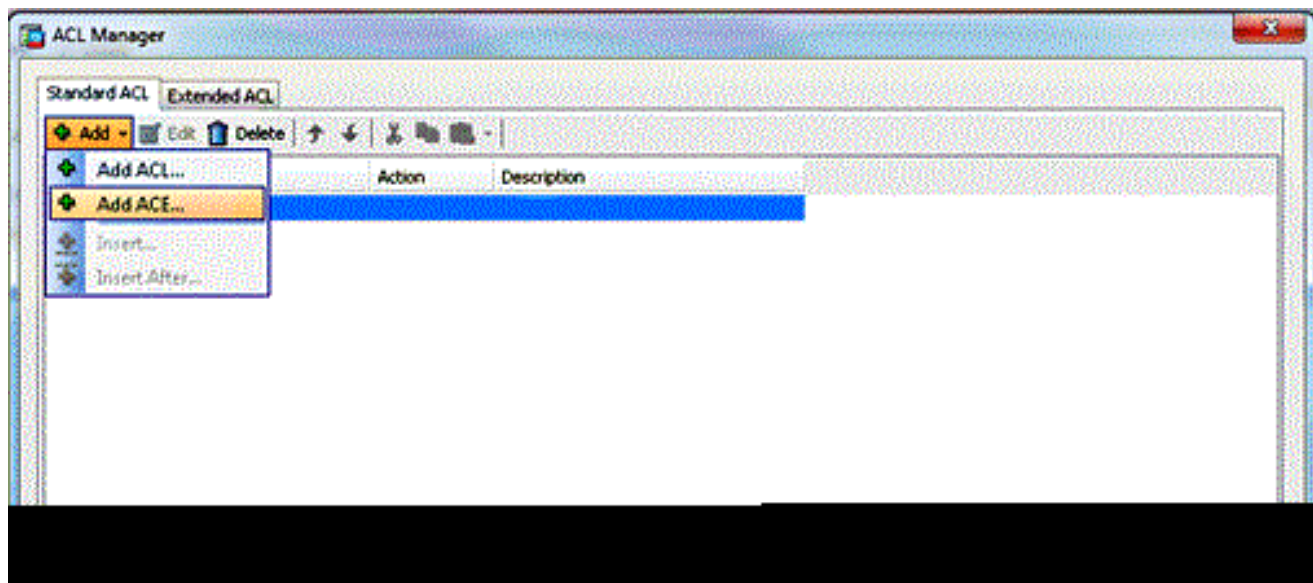
- ACL Managerで、新しいアクセスリストを作成するために Add > Add ACL... を選択します。



- ACLの名前を指定して、OKをクリックします。



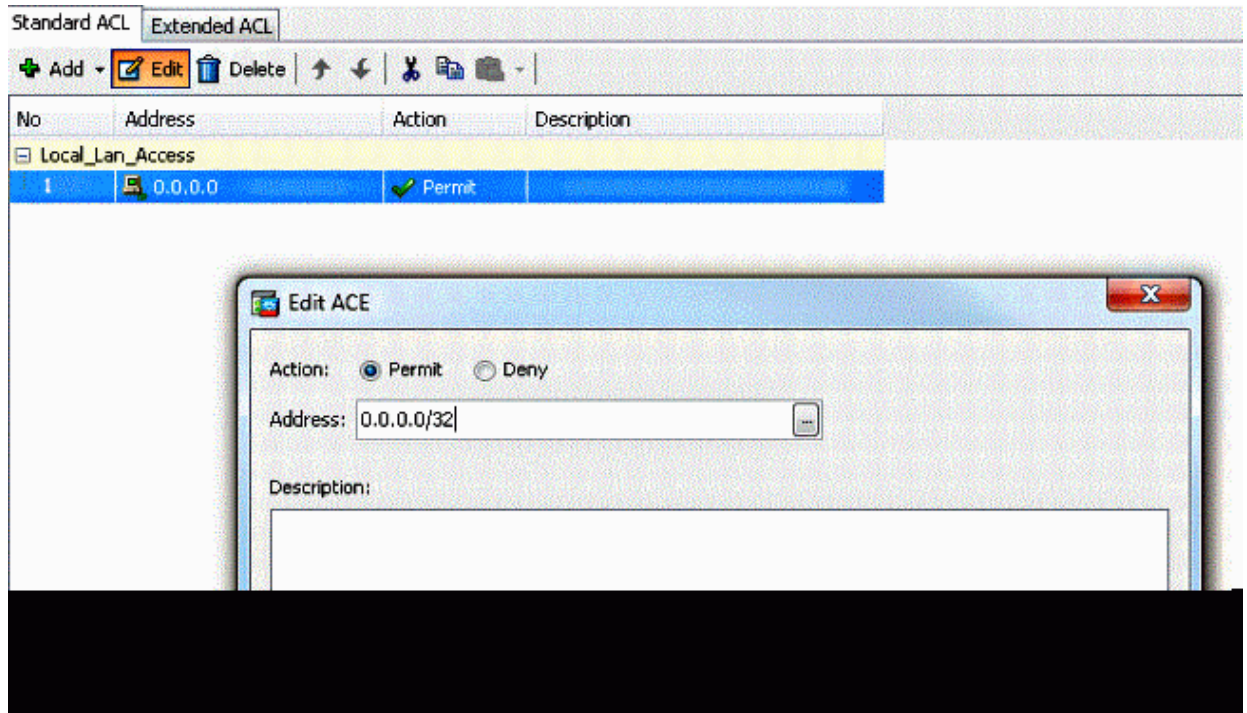
- ACLを作成したら、**Add > Add ACE...** を選択して、アクセスコントロールエントリ(ACE)を追加します。



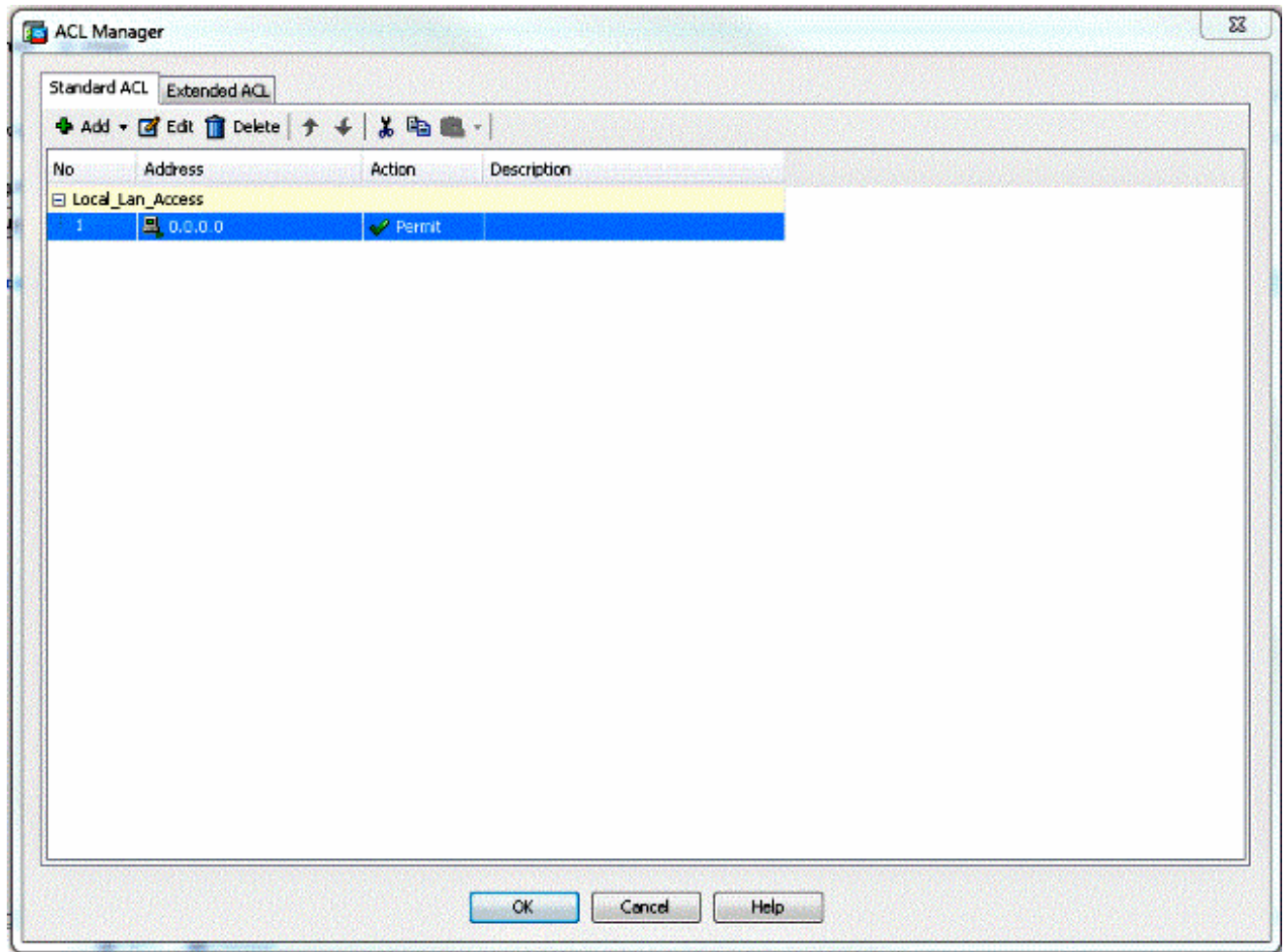
- クライアントのローカル LAN に対応する ACE を定義します。

a. 選択. **Permit**

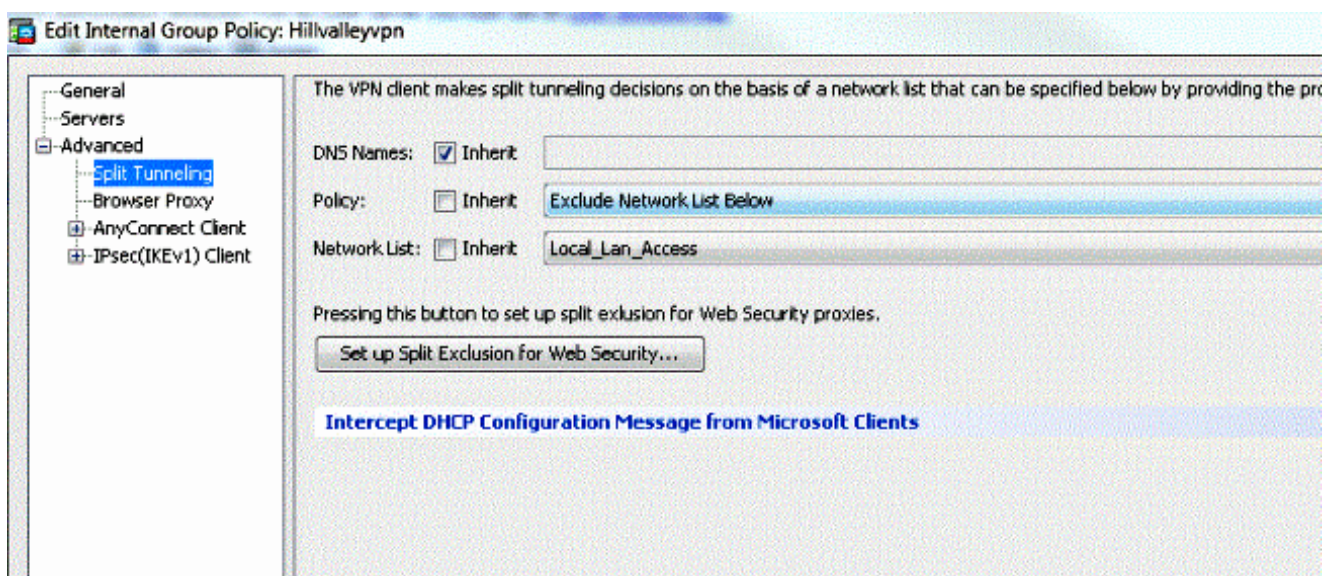
- IP アドレス 0.0.0.0 を選択します。
- /32 のネットマスクを選択します。
- (任意) 説明を入力します。
- をクリックします。 **OK**



- **OK** をクリックして、ACL Managerを終了します。



- Split Tunnel Network List で、作成した ACL が選択されていることを確認します。



- **OK** をクリックして、グループポリシーの設定に戻ります。

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameter

DNS Names: Inherit

Policy: Inherit Exclude Network List Below

Network List: Inherit Local_Lan_Access

Pressing this button to set up split exclusion for Web Security proxies.

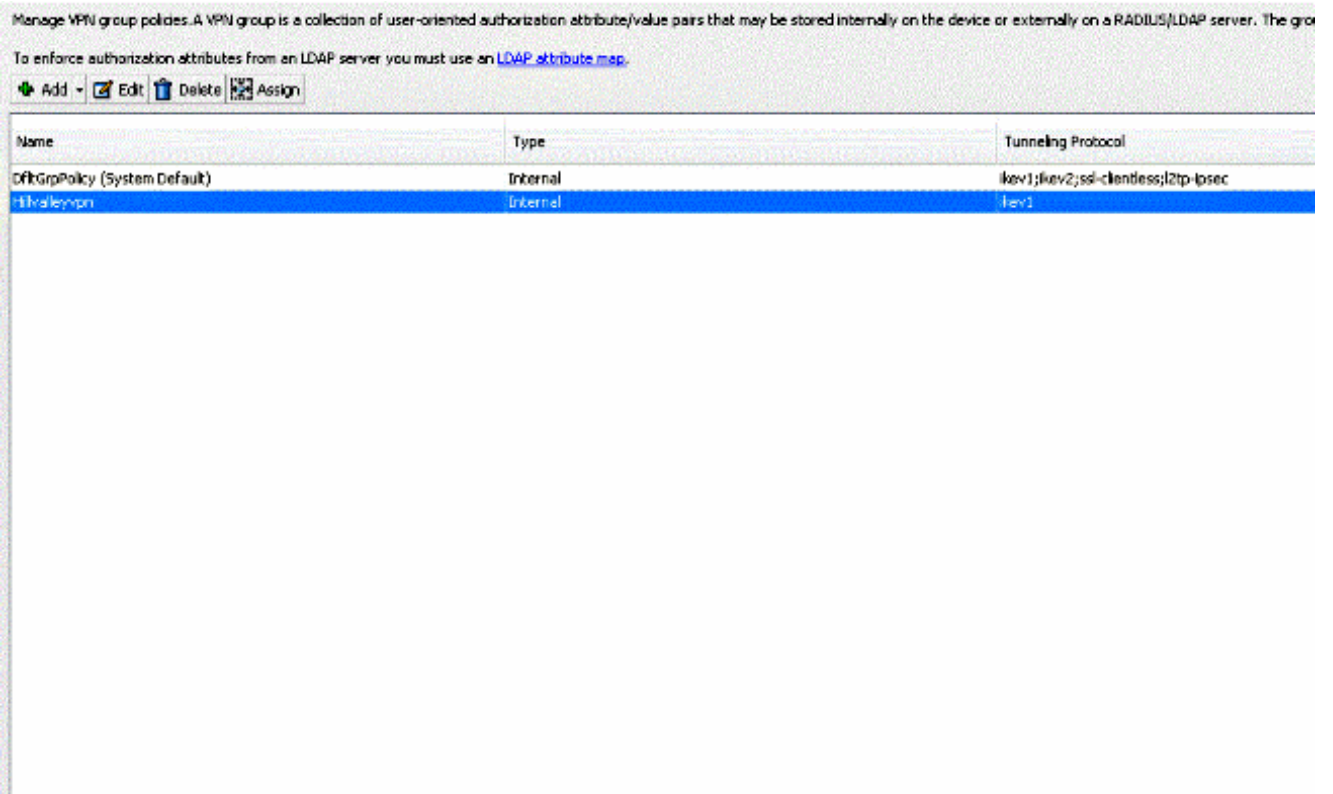
Set up Split Exclusion for Web Security...

Intercept DHCP Configuration Message from Microsoft Clients

Next Previous

OK Cancel Help

- **Apply** をクリックし、必要に応じて **Send** をクリックしてコマンドをASAに送信します。



CLIによる ASA の設定

ASA に接続しているときに VPN Client にローカル LAN へのアクセスを許可するには、ASDM を使用する代わりに ASA CLI で次の手順を実行することもできます。

- コンフィギュレーション モードに切り替えます。

```
<#root>
```

```
ciscoasa>
```

enable

Password:
ciscoasa#

configure terminal

ciscoasa(config)#

- ローカル LAN アクセスを許可するアクセス リストを作成します。

<#root>

ciscoasa(config)#

```
access-list Local_LAN_Access remark Client Local LAN Access
```

ciscoasa(config)#

```
access-list Local_LAN_Access standard permit host 0.0.0.0
```

- 修正するポリシーのグループ ポリシー コンフィギュレーション モードに入ります。

<#root>

ciscoasa(config)#

```
group-policy hillvalleyvpn attributes
```

```
ciscoasa(config-group-policy)#
```

- スプリット トンネル ポリシーを指定します。この場合、ポリシーは `excludespecified`です。

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
split-tunnel-policy excludespecified
```

- スプリット トンネル アクセス リストを指定します。この場合、リストは `Local_LAN_Access`です。

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
split-tunnel-network-list value Local_LAN_Access
```

- 次のコマンドを実行します。

```
<#root>
```

```
ciscoasa(config)#
```

```
tunnel-group hillvalleyvpn general-attributes
```

- グループポリシーをトンネルグループに関連付けます。

```
<#root>
```

```
ciscoasa(config-tunnel-ipsec)#
```

```
default-group-policy hillvalleyvpn
```

- 2つのコンフィギュレーション モードを終了します。

```
<#root>
```

```
ciscoasa(config-group-policy)#
```

```
exit
```

```
ciscoasa(config)#
```

```
exit
```

```
ciscoasa#
```

- 設定を不揮発性RAM(NVRAM)に保存し、ソースファイル名を指定するようにプロンプトが表示されたら、Enter を押します。

```
<#root>
```

```
ciscoasa#
```

```
copy running-config startup-config
```

```
Source filename [running-config]?  
Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a  
  
3847 bytes copied in 3.470 secs (1282 bytes/sec)  
ciscoasa#
```

Cisco AnyConnect セキュア モビリティ クライアントの設定

Cisco AnyConnectセキュアモビリティクライアントを設定するには、『[CLIブック3: Cisco ASAシリーズVPN CLIコンフィギュレーションガイド、9.17](#)』の「AnyConnect接続の設定」セクションを参照してください。

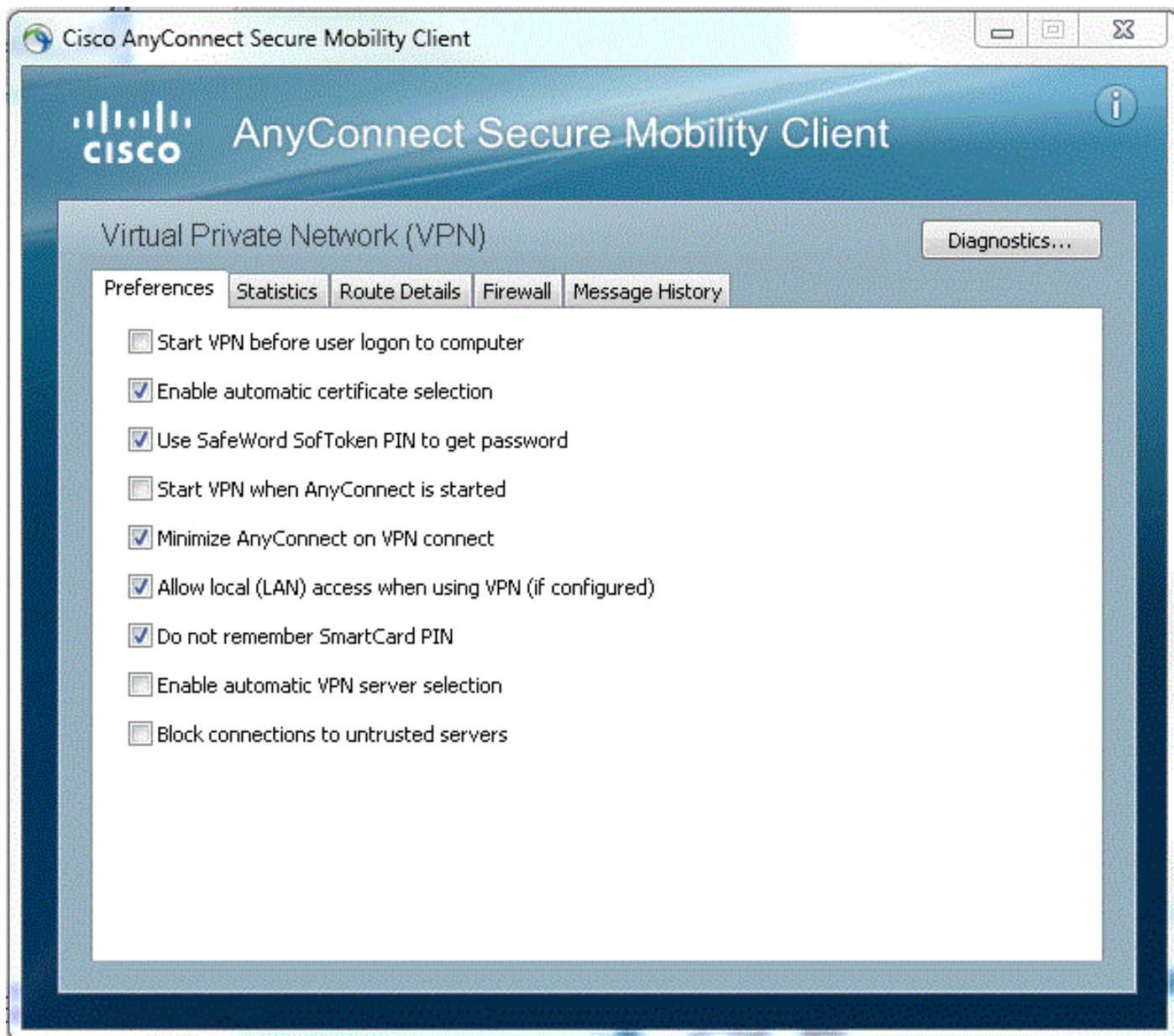
スプリット除外トンネリングでは、AnyConnectクライアントで **AllowLocalLanAccess** をイネーブルにする必要があります。すべてのスプリット除外トンネリングは、ローカル LAN アクセスと見なされます。スプリットトンネリングの除外機能を使用するには、AnyConnect VPN Client preferencesで **AllowLocalLanAccess** プリファレンスをイネーブルにする必要があります。デフォルトでは、ローカル LAN アクセスはディセーブルになっています。

ローカル LAN アクセスを許可し、そのためにスプリット除外トンネリングを許可するには、ネットワーク管理者がそれをプロファイル内で有効にするか、ユーザがプリファレンス設定で有効にすることができます (次のセクションの画像を参照してください)。スプリットトンネリングがセキュアゲートウェイ上で有効になっており、ポリシーを使用して設定されている場合、ローカル LAN アクセスを許可するためにユーザが **Allow Local LAN access** エックボックスを **split-tunnel-policy exclude specified** にします。また、`<LocalLanAccess UserControllable="true">true</LocalLanAccess>` を使用してローカル LAN アクセスが許可されている場合は、VPN Clientプロファイルを設定できます。

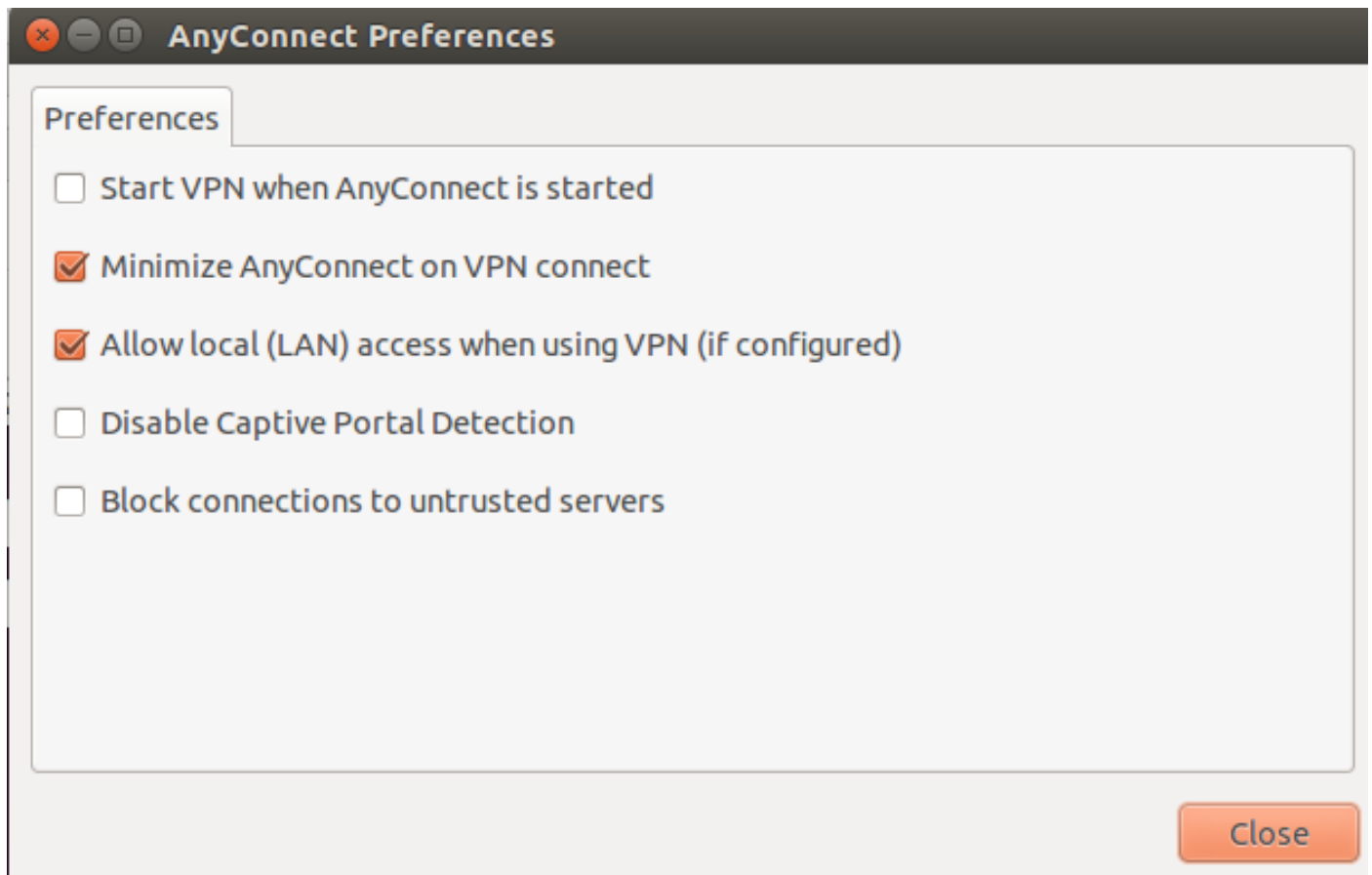
ユーザ設定

ローカル LAN アクセスを許可するためにCisco AnyConnectセキュアモビリティクライアントのPreferencesタブで行う必要がある選

択を次に示します。



Linux上



XML プロファイルの例

次に、XML で VPN クライアント プロファイルを設定する例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSA SecurIDIntegration UserControllable="false">Automatic
```

```
</RSA SecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPEXclusion UserControllable="false">Disable
<PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
</PPPEXclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">>false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>>false
</RetainVpnOnLogoff>
</ClientInitialization>
</AnyConnectProfile>
```

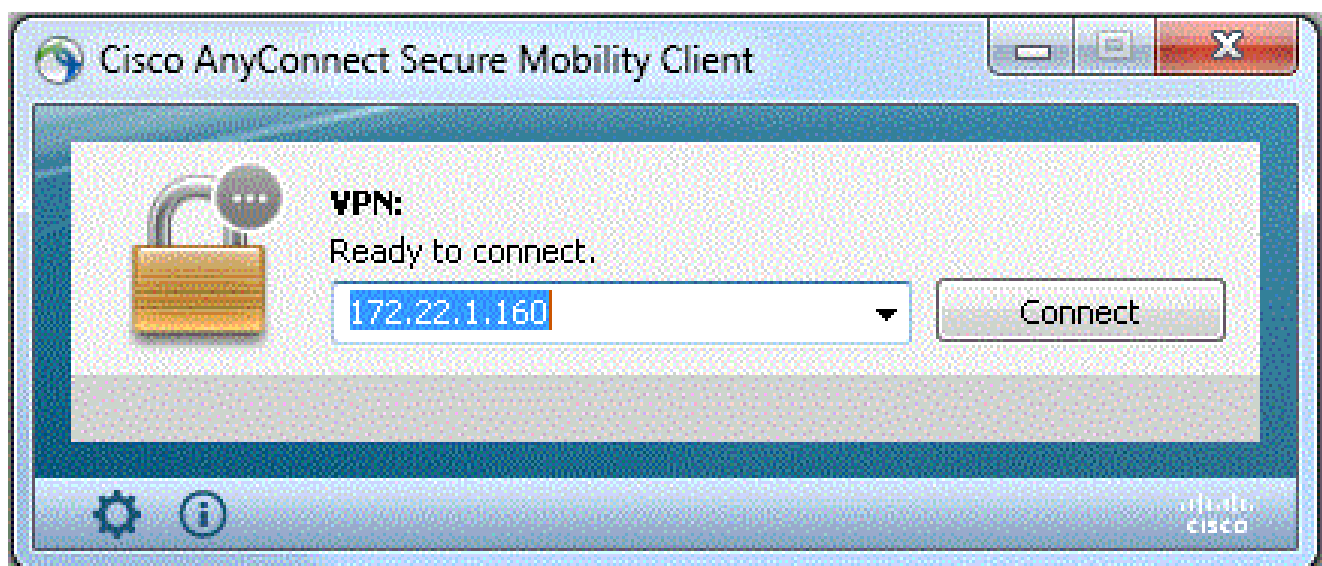
確認

設定を確認するには、次のセクションの手順を実行します。

- [DART の表示](#)
- [Ping でローカル LAN アクセスをテストする](#)

Cisco AnyConnect セキュア モビリティ クライアントを ASA に接続して設定を検証します。

- サーバリストから接続エントリを選択し、**Connect**をクリックします。



- Advanced Window for All Components > Statistics... を選択して、トンネルモードを表示します。

Virtual Private Network (VPN)

Statistics | Route Details | Firewall | Message History


Connection Information		Address Information	
State:	Connected	Client (IPv4):	192.168.11.1
Tunnel Mode (IPv4):	Split Exclude	Client (IPv6):	Not Available
Tunnel Mode (IPv6):	Drop All Traffic	Server:	64.102.156.87
Duration:	00:01:11	Transport Information	
Bytes		Protocol:	DTLS
Sent:	49749	Cipher:	RSA_3DES_168_SHA1
Received:	9298	Compression:	LZS
Frames		Proxy Address:	No Proxy
Sent:	710	Feature Configuration	
Received:	3	FIPS Mode:	Disabled
Control Frames		Trusted Network Detection:	Disabled
Sent:	7	Always On:	Disabled
Received:	5	Secure Mobility Solution	
Client Management		Status:	Unconfirmed
Profile Name:	pro_locallan.xml	Appliance:	Not Available
Administrative Domain:	Undefined		

Reset Export Stats...

Linux上

Cisco AnyConnect Secure Mobility Client Statistics

Statistics | Route Details



Connection Information		Address Information	
State:	Connected	Client (IPv4):	20.20.20.1
Connection Mode (IPv4):	Split Exclude	Server:	10.48.67.223
Connection Mode (IPv6):	Drop All Traffic	Client (IPv6):	Not Available
Duration:	00:16:22		
Session Disconnect:	None		
Bytes		Transport Information	
Sent:	0	Protocol:	DTLS
Received:	20550	Cipher:	RSA_AES_256_SHA1
		Compression:	None
		Proxy Address:	No Proxy
Frames		Feature Configuration	
Sent:	0	FIPS Mode:	Disabled
Received:	5	Trusted Network Detection:	Disabled
Control Frames			
Sent:	132		
Received:	65		

- Cisco AnyConnectセキュアモビリティクライアントがローカルアクセスできるルートを表示するには、 **Route Details** タブをクリックします。


この例では、クライアントは 10.150.52.0/22 および 169.254.0.0/16 へのローカル LAN アクセスを許可されています。その他のすべてのトラフィックは暗号化され、トンネル経由で送信されます。



Linux上

Cisco AnyConnect Secure Mobility Client Statistics

Statistics | **Route Details**



Non-Secured Routes		Secured Routes	
Destination	Subnet Mask	Destination	Subnet Mask
192.168.171.0	24	0.0.0.0	0

Cisco AnyConnect セキュア モビリティ クライアント

Diagnostics and Reporting Tool (DART) から AnyConnect ログを調べると、ローカル LAN アクセスを許可するパラメータが設定されているかどうかを判断できます。

Date : 11/25/2011
 Time : 13:01:48
 Type : Information
 Source : acvpndownloader

Description : Current Preference Settings:
 ServiceDisable: false
 CertificateStoreOverride: false
 CertificateStore: All
 ShowPreConnectMessage: false
 AutoConnectOnStart: false
 MinimizeOnConnect: true
 LocalLanAccess: true
 AutoReconnect: true
 AutoReconnectBehavior: DisconnectOnSuspend
 UseStartBeforeLogon: false
 AutoUpdate: true
 RSA SecurID Integration: Automatic
 Windows Logon Enforcement: SingleLocalLogon
 Windows VPN Establishment: LocalUsersOnly
 Proxy Settings: Native
 AllowLocalProxyConnections: true

PPPEXclusion: Disable
PPPEXclusionServerIP:
AutomaticVPNPolicy: false
TrustedNetworkPolicy: Disconnect
UntrustedNetworkPolicy: Connect
TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: false
ConnectFailurePolicy: Closed
AllowCaptivePortalRemediation: false
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: false
AllowVPNDisconnect: true
EnableScripting: false
TerminateScriptOnNextEvent: false
EnablePostSBLOnConnectScript: true
AutomaticCertSelection: true
RetainVpnOnLogoff: false
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: false
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSoftTokenIntegration: false
AllowIPsecOverSSL: false
ClearSmartcardPin: true

Ping でローカル LAN アクセスをテストする

VPN ClientがVPNヘッドエンドとトンネル接続しながらローカルLANアクセスが維持できているかどうかは、Microsoft Windowsコマンドラインで **ping** コマンドを発行する方法でもテストできます。クライアントのローカル LAN が 192.168.0.0/24 で、もう一方のホストも同じネットワーク上に存在し、IP アドレス 192.168.0.3 が付与されている例を次に示します。

<#root>

C:\>

ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

```
malhyari@ubuntu:~$ ping 192.168.171.131
PING 192.168.171.131 (192.168.171.131) 56(84) bytes of data.
64 bytes from 192.168.171.131: icmp_seq=1 ttl=128 time=0.474 ms
64 bytes from 192.168.171.131: icmp_seq=2 ttl=128 time=0.315 ms
64 bytes from 192.168.171.131: icmp_seq=3 ttl=128 time=0.336 ms
64 bytes from 192.168.171.131: icmp_seq=4 ttl=128 time=0.475 ms
64 bytes from 192.168.171.131: icmp_seq=5 ttl=128 time=0.337 ms
64 bytes from 192.168.171.131: icmp_seq=6 ttl=128 time=0.286 ms
64 bytes from 192.168.171.131: icmp_seq=7 ttl=128 time=0.252 ms
```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

名前による印刷またはブラウズができない

VPN Client がローカル LAN アクセス用に接続され設定されていると、ローカル LAN では名前によって印刷やブラウズを行うことはできません。この状況を回避するために次の2つのオプションを利用できます。

- IP アドレスでブラウズまたは印刷する。
 - ブラウズするには、構文 `\\sharename` ではなく、`\\x.x.x.x(x.x.x.xはホストコンピュータのIPアドレス)`を使用します。
 - 印刷する場合は、ネットワーク プリンタのプロパティを変更して、名前の代わりに IP アドレスを使用するように設定します。たとえば、構文「`\\sharename\printername`」の代わりに「`\\x.x.x.x\printername`」を使用します。`x.x.x.x`にはIPアドレスを指定します。
- VPN クライアントの LMHOSTS ファイルを作成または修正します。Microsoft Windows PC 上の LMHOSTS ファイルによって、ホスト名と IP アドレスの間のスタティック マッピングを作成できます。たとえば、LMHOSTS ファイルは次のようになります。

```
192.168.0.3 SERVER1
192.168.0.4 SERVER2
192.168.0.5 SERVER3
```


Microsoft Windows XP Professional Editionでは、LMHOSTSファイルは %SystemRoot%\System32\Drivers\Etcにあります。詳細については、Microsoftのマニュアルを参照してください。

関連情報

- [CLIブック3: Cisco ASAシリーズVPN CLIコンフィギュレーションガイド9.17](#)
- [Cisco ASA 5500-Xシリーズファイアウォール](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。